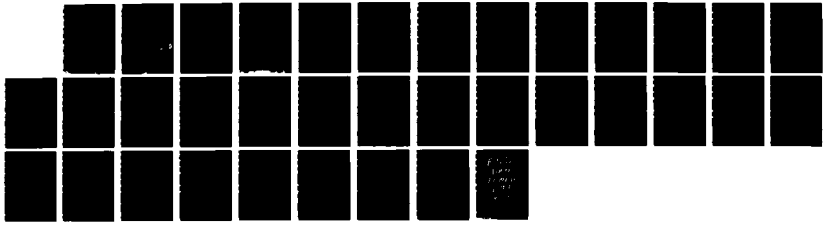
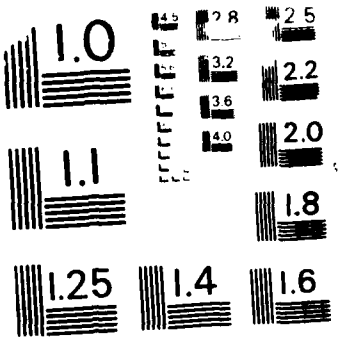
AD-A198 422 APPLICATIONS OF SIGNAL PROCESSING IN DIGITAL COMMUNICATIONS(U) POLITECNICO DI TORINO (ITALY) DEPT DI ELETTRONICA M ELIA 18 NOV 87 R/D-5228-CC-03 1/1

UNCLASSIFIED DAJA45-86-C-0044 F/G 12/9 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

R&D-5228-CC-03

(2)

AD-A190 422

APPLICATIONS OF SIGNAL PROCESSING

IN DIGITAL COMMUNICATIONS

Principal Investigator: Michele Elia

Contractor: Politecnico di Torino
Corso Duca degli Abruzzi 24 - I-10129 TORINO (Italy)

Contract number DAJA45-86-C-0044

Third Interim Report
(May 1987 - October 1987)

DTIC
ELECTE
FEB 1 6 1988
S D
E

The Research reported in this document has been made possible through the support and sponsorship of the U.S. Government through its European Research Office of the U.S. Army. ~~This report is intended only for the internal management use of the Contractor and the U.S. Government~~.

This document has been approved for public release and sale; its distribution is unlimited.

Our research activity during the period covered by this report was focused on the design of signal constellations to be used in trellis codes.
The increased importance of combined codes and modulations have resorted a wide interest in group codes for Gaussian channel, first introduced by Slepian, and in the more recent concept of generalized group alphabet.

Our main aim was to collect and organize the principal results in this area in order to present a state of the art in group coding theory. As a consequence some new point configurations were found and their properties exploited.

The paper herewith enclosed, includes a review of group codes theory as well as new point configurations which appear promising for the applications.
The paper was presented at the International Symposium on Information and Coding Theory held in Campinas - SP - Brazil, from July 27 to August 3, 1987.

Accession For	
NTIS GRA&I	☒
DTIC TAB	☐
Unannounced	☐
Justification per form 50	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

QUALITY INSPECTED 2

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

REPORT DOCUMENTATION PAGE		READ INSTRUCTIONS BEFORE COMPLETING FORM
1. REPORT NUMBER	2. GOVT ACCESSION NO.	3. RECIPIENT'S CATALOG NUMBER
4. TITLE (and Subtitle) Applications of Signal Processing in Digital Communications		5. TYPE OF REPORT & PERIOD COVERED (May 1987 - October 1987) Interim Report
		6. PERFORMING ORG. REPORT NUMBER
7. AUTHOR(s) Michele Elia		8. CONTRACT OR GRANT NUMBER(s) DAJA45-86-C-0044
9. PERFORMING ORGANIZATION NAME AND ADDRESS Dipartimento di Elettronica Politecnico di Torino Corso D. Abruzzi 24 - I10129 Torino (I)		10. PROGRAM ELEMENT, PROJECT, TASK AREA & WORK UNIT NUMBERS
11. CONTROLLING OFFICE NAME AND ADDRESS U.S.Army Research, Development & Standardization GRoup - UK		12. REPORT DATE November 10, 1987 13. NUMBER OF PAGES 31
14. MONITORING AGENCY NAME & ADDRESS(if different from Controlling Office)		15. SECURITY CLASS. (of this report) Unclassified 15a. DECLASSIFICATION/DOWNGRADING SCHEDULE

16. DISTRIBUTION STATEMENT (of this Report)

17. DISTRIBUTION STATEMENT (of the abstract entered in Block 20, if different from Report)

18. SUPPLEMENTARY NOTES

19. KEY WORDS (Continue on reverse side if necessary and identify by block number)

Digital Communications, Group Codes,

20. ABSTRACT (Continue on reverse side if necessary and identify by block number)

We consider the design of multidimensional signal sets and their combination with block or trellis codes. The goal is to achieve a high efficiency in the use of frequency spectrum for digital communications.

DD FORM 1 JAN 73 1473 EDITION OF 1 NOV 65 IS OBSOLETE

SECURITY CLASSIFICATION OF THIS PAGE (When Data Entered)

GROUP CODES AND SIGNAL DESIGN FOR DIGITAL TRANSMISSION

by

Michele Elia

Dipartimento di Elettronica - POLITECNICO DI TORINO - ITALY

I - INTRODUCTION

Symmetry seems to be a feature intrinsic to every life process. It should be a very stimulating undertaking to discuss the fundamental role played by symmetry in art, music, chemistry, biology, physics, computer science and more generally in every mathematical science. A fascinating sample of this subject was provided by H. Weyl [53] in his last book dedicated to a synthetic view of symmetry. Nevertheless in this paper we limit our considerations to the key role of symmetry in communication theory. In this field symmetry plays an indispensable part in reducing the complexity of every data transmission scheme.

The algebraic notion of group underlies both the geometrical description of digital signals proposed by Shannon, [43], and the geometrical methods of error control codes developed shortly after Shannon's work. However the introduction and systematic use of methodology, machinery and language of group theory in both coding theory and signal design must be ascribed to Slepian [2,3].

In some way Slepian's approach parallels Klein's Erlagen program on the foundation of geometry: all geometric objects and concepts can be formulated starting from the abstract notion of group which provides

---

This work has been sponsored in part by the United States Army through its European Research Office grant N. DAJA45-86-C-0044, and in part by Consiglio Nazionale delle Ricerche through grant N. 86.02428.07.

the appropriate tool for every useful and applied mathematical theory. In Klein's words "a geometry is defined by a group of transformations, and investigates everything that is invariant under the transformations of the given group". In our context the main object left invariant by the group is a code, as will be defined later.

The Shannon theory of any communication process shows that the information is inherently discrete and also that the quantity of information that can be processed by every practical system is finite.

Signals for sending information over physical channels are essentially time- and frequency-limited; as a consequence the dimension of the signal space is finite. The signal energy, defined as the integral of the signal square over its finite time interval, induces an euclidean metric in this signal space. Therefore, by using an orthonormal basis, we associate to each signal a point (or vector) in an euclidean finite dimensional space. In this way a finite set of signals corresponds to a finite constellation of points that we call a code.

Early in the fifties Slepian introduced the concept of group code in the design of signal sets for the Gaussian channel. A group code is a set of M unit vectors spanning an n-dimensional real space, on which the matrices of a finite group representation operate transitively.

A straightforward generalization of Slepian's group codes is obtained by considering a set of initial vectors instead of just one vector. The resulting set of vectors is called generalized group alphabet.

The present awakening of interest in group codes is due to their increasing use in transmission schemes of combined modulation with either convolutional or block codes, an approach initiated by Ungerboeck.

A fundamental problem for Slepian's group codes is the choice of the initial vector that maximizes the minimum distance. A second basic problem concerns the existence of group codes for every pair of integers with M greater than n. The classification of all configurations of given dimension is constructively important. As far as we know, only the classification in dimension three is complete. The same problems, formulated for generalized group alphabets, seem even more difficult.

However the field is wide and deserves investigations either from a purely theoretical point of view or for practical applications.
We are aware of the fact that the theory of group codes is still incomplete, but the open problems really challenge the human thinking and stimulate the research work of engineers and mathematicians alike.

II - SIGNAL SETS: THE GEOMETRICAL MODEL

Signals for sending information are essentially limited both in time and frequency. According to a point of view accepted in the past, the simultaneous concentration attainable in both domains is limited by an uncertainty principle, so named after the analogous relations in quantum mechanics. Moreover energy constraints are imposed for practical purposes.
Finite bandwidth W and finite time duration T together imply that the dimension of the Hilbert space of the signals is essentially finite.
If we require strictly finite duration and simultaneously maximum concentration of signal energy in a given bandwidth, we have a problem whose natural mathematical setting is the calculus of variations. This problem has been thorougly discussed, [30,5,40,41], even if its consequences have not received much attention from the signal designers yet.
Let V be a Hilbert space with support the interval [0,T], and let the scalar product be defined as

$$(\varphi,\psi) = \int_0^T \varphi(t)\,\overline{\psi(t)}\,dt \qquad \varphi(t),\ \psi(t)\in V$$

where overbar denotes complex conjugation.
The norm square $\|.\|^2$, defined as $\|\varphi\|^2 = (\varphi,\varphi)$ represents the energy of the signal $\varphi(t)\in V$. In the set of linear operators acting in V and having a discrete spectrum, the operators associated to linear filters

are of particular interest. Let $H(f)$ denote the filter transfer function. Therefore the Fourier transforms $\Phi(f)$ and $\Psi(f)$, respectively of filter input and output signal, are related by

$$\Psi(f) = H(f)\,\Phi(f) \quad .$$

The problem now is to seek the input function $\varphi(t)$, of unit energy, for which the energy of the corresponding output functions $\psi(t)$, in the bandwidth $[-W,W]$, is as large as possible. That is, we want to maximize the following integral

$$I_1 = \int_{-W}^{W} \Psi(f)\,\overline{\Psi(f)}\,df = \int_{-W}^{W} H(f)\,\overline{H(f)}\,\Phi(f)\,\overline{\Phi(f)}\,df$$

under the constraint

$$I_2 = \int_{-\infty}^{\infty} \Phi(f)\,\overline{\Phi(f)}\,df = 1 \quad .$$

By means of Lagrange's multipliers the solution is found to be the eigenfunction associated to the largest eigenvalue of the integral equation

$$(1) \qquad \int_{0}^{T} K(t-s)\,\varphi(s)\,ds = \lambda\,\varphi(t) \qquad t\in[0,T]$$

where the positive definite kernel is defined by the Fourier transform

$$K(t-s) = \int_{-W}^{W} H(f)\overline{H(f)}\,\exp[2\pi j(t-s)f]\,df.$$

The positive eigenvalues λ, ordered in decreasing order, exhibit the typical trend shown in Fig.1, which demonstrates that the dimension of the signal space of functions limited both in time and frequency is essentially finite and can be taken to be approximately 2WT, [5]. (If $2TW>10$, this statement is true within an energy dispersion of some few per cent and irrespective of $H(f)$).

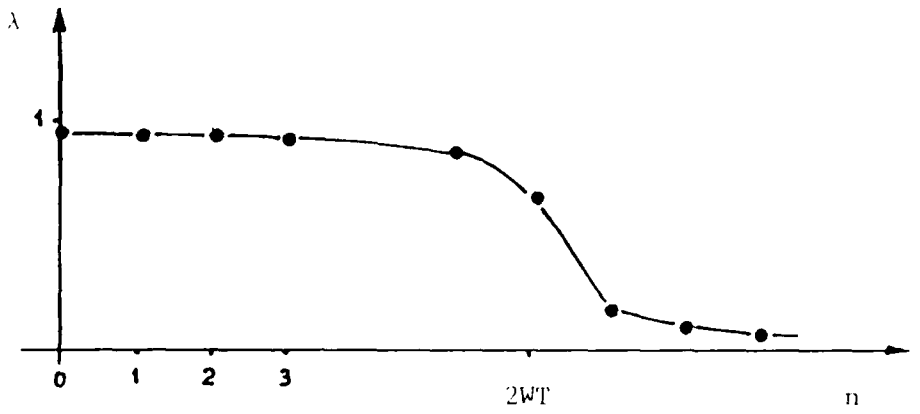


Fig.1 - Typical behavior of the eigenvalues of equation (1)

A natural orthogonal basis $B = \{\psi_i(t)\}_{i=1}^{n}$, $n \leq 2WT$, for the space of the signals limited both in time and frequency is provided by the set of normalized eigenfunctions associated to the set of eigenvalues of greatest value. By means of the basis B, we can uniquely associate to a given set A of M signals

$$m_i(t) = \sum_{j=1}^{n} x_{ij}\ \psi_j(t) \qquad i=1, \ \ldots\ , M$$

a set $\mathbb{C}$ of M vectors

$$X_i=(x_{i1}, \ \ldots\ , \ x_{in}) \qquad i=1, \ \ldots\ , M \ .$$

that we call code. The square of the Euclidean length of a vector X is equal to the energy of the signal m(t).

We can now describe the operation of a quite general model of transmission scheme at the level of signal manipulation.

A transmitter associates to every source symbol, in a one-to-one way, a signal chosen in the set A and sends this signal through the channel.

The channel operates by adding to the transmitted waveform m(t) a sample of a zero-mean random process $\nu(t)$ with known spectral density.

The received signal is thus

$$r(t) = m_\xi(t) + \nu(t) \qquad t\in[0,T]$$

where ξ is a random variable taking values in the set $\{1,\ldots,M\}$.

If we confine ourselves to coherent detection, from the observation of r(t) over the interval [0,T], the receiver makes an estimate of the value taken by ξ, that is, an estimation of the symbol emitted by the

source. Let us suppose that all the information relevant to every detection criterion lies in the signal space, therefore any decision can be taken by referring to the vector

$$\underline{r}=(r_1, \ldots, r_n)$$

where

$$r_i= \int_0^T r(t)\, \overline{\psi_i(t)}\, dt \quad .$$

This is equivalent to considering a discrete-time continuous-amplitude additive channel that produces

$$\underline{r} = \underline{X}_\xi + \underline{N}$$

where: $\underline{N}$ is a random vector with known probability density f(.);

$\underline{X}_\xi$ is a transmitted code vector from the code $\mathbb{C}$.

At the receiver end, the decision taker may be described by an exhaustive partition of the n-dimensional space into M' disjoint regions R_i, i=1,...,M', if the received vector $\underline{r}$ falls in region R_j then the detected symbol will correspond to the integer j. We say that the demodulator takes a "hard" decision or a "soft" decision depending on whether M'=M or M'>M respectively. In conclusion the channel is modelled by a discrete memoryless channel with M input symbols and M' output symbols.

III - MEASURES OF PERFORMANCE

The performance evaluations of group codes on communication channels rule the development of the entire theory of group codes. Hereafter we briefly review some important performance indices used in digital communication systems. In order to avoid discussions depending on transmission protocols, here and in the following we will deal only with transmission schemes based on hard decisions. In this context the most typical index is error probability, i.e. the probability that the receiver takes a wrong decision about the symbol emitted by the infor-

mation source. Assuming in particular equienergetic codes, white Gaussian noise channel and maximum likelihood decision criterion at the receiver's end, then the regions R_i, i=1,...,M, will be connected hypercones bounded by hyperplanes with the vertices in the origin. Therefore the error probability is given by a sum of n-dimensional integrals; letting $\hat{R}_i$ denote the complementary region of R_i in R^n and let $p\{X_i\}$ be the probability of sending message i, we have

$$p(e) = \sum_{i=1}^{M} \int_{\hat{R}_i} f(X-X_i)\, dX\, p\{X_i\} \quad .$$

A second important index is the configuration matrix $C=(c_{ij})$ defined as the Gram matrix of the set of vectors, i.e.

$$c_{ij} = X_i^T X_j \quad .$$

This matrix C occupies a central position in the theory of group codes. It conveys all the information relevant to evaluate code performances on the white Gaussian channel and is also useful to compute other performance indices.

A third relevant index is the minimum distance defined as the minimum distance between any pair of distinct vectors of the code, that is

$$d^2_{min} = \min_{i \neq j} \| X_i - X_j \|^2 \quad .$$

The evaluation of each performance index is usually very hard, so that frequently the knowledge of upper and/or lower bounds is of sufficient interest. As an example we derive an upper bound for the error probability, that applies to symmetric point configurations.

Let us assume that the code has a symmetry such that the error probabilities conditioned on a given code vector do not depend on this vector, i.e. $p\{e\} = p\{e|X_i\}$ $\quad i=1,\ldots,M$

Let the region R_i, i=1,...,M, be bounded by the set of s hyperplanes of equations $\|X-X_i\|^2 = \|X-X_j\|^2$

where j belongs to a convenient subset of $\{1,\ldots,M\}$; the explicit equation of each hyperplane turns out to be $X^T(X_i-X_j) = 0$.
Applying the union bound, we get a general upper bound for the error probability

$$p(e) = p\{e|X_i\} = \int_{\hat{R}_i} f(X-X_i)\,dX < \sum_{j=1}^{s} \int_{\Omega_j} f(X-X_i)\,dX$$

$$\leq s \int_{\Omega_o} f(X-X_1)\,dX$$

where Ω_j is the halfspace defined by the inequality $X^T(X_i-X_j) \leq 0$.

Ω_o is the halfspace defined by the inequality $X^T(X_1-X_o) \leq 0$.

and X_o is a code vector at the minimum distance from X_1.

More detailed comments on performance indices will be provided after the description of the main features of group codes.

IV - GROUP CODES

Symmetry seems to be an unavoidable occurrence for reducing the complexity of every high-dimensional set of signals as required by Shannon's channel theorem to guarantee high coding performance. For instance, we can take advantage of symmetry in designing good decoding algorithms for error control codes. Symmetry makes feasible the new digital modulation schemes which combine error control codes and modulations.
As we observed in the introduction, symmetry cannot be separated from the notion of group which discloses symmetry's real nature and constitutes its formal counterpart. It was early in the fifties that Slepian introduced the group codes for Gaussian channels; his ideas found a definitive formulation in a stimulating paper [3], in 1965.

Now let us formally define the main object of this paper.

Definition 1.

Consider a finite set $S(G) = \{D(g): g\in G\}$ of real orthogonal matrices that form a faithful representation of a finite group G and consider an n-dimensional unit vector X_1. The set $S(G)X_1 = \{X_g=D(g)X_1 : g\in G\}$ of M vectors generated by the action of S(G) on X_1 is called group code and denoted by [M,n], if it spans the n-dimensional space; otherwise it is called planar group code.

In the present theory, group representations by matrices having real entries are a fundamental mathematical tool.

The theory of group representations originated in the middle of the nineteenth century from the works of many mathematicians. Equipped with the theory of group characters, (the character of $g\in G$ is the trace of the matrix D(g)), the theory of matrix groups assumed a central role in the development of modern algebra. We do not try to survey this subject. To coding theorists we recommend the book by Blake and Mullin [12], while for a thorough development of the topic we refer to the books by Curtis and Reiner [24], Burrow [17] and van der Waerden [48]. Old fashioned but very rich and suggestive is the book by Burnside, [16].

For easy reference and later use we recall some results concerning group representations.

1 - A group representation is either irreducible or completely reducible, i.e. it can be written as direct sum of irreducible components.

2 - A representation with real entries may be either real reducible, or real irreducible. In this second case it may still be complex reducible or not.

3 - The number of distinct irreducible components is equal to the number of group classes.

4 - Given two representations of groups G and G_1 we obtain a representation of their direct product by means of the direct matrix sum

$D(g\ g') = D(g) \oplus D(g')$ $\qquad g \in G$ and $g' \in G_1$

The concept of direct matrix sum is very important in describing the structure of group codes. The general observation fits a paradigmatic principle: in many instances to split a problem means to solve it.
Let $|G|$ denote the cardinality of the group G. The cardinality M of the code may be less than or equal to $|G|$. In case it is less there exists a subgroup H of G such that the initial vector is left invariant, i.e.

$$HX_1 = X_1$$

where with HX_1 we denote the set $\{X: X = D(h)X_1 , h \in H\}$.
The proof of the following theorem is straightforward and follows from definition 1 and elementary properties of the groups.

Theorem 1.

i) $|G| \geq M$ and $|G| \mid M!$

ii) if $|G| > M$ then $M \mid |G|$

where $d|b$ means that d is a divisor of b.

The following theorem concerning the subgroup H, has an important consequence on the existence conditions for group codes. It is also useful to clarify the relations between the group and the code.

Theorem 2.

The subgroup H cannot be normal.
See [7, 12, 35] for a proof.

Theorem 3.

If G is abelian then $|G| = M$.

Besides the abstract properties of the group G, also conditions concerning the skeleton of its representations are important for distinguishing between planar and non planar codes.
In order that an initial vector exists such that the generated set of vectors spans the n-dimensional space, the representations of the group G must satisfy the condition expressed in the following theorem.

Theorem 4.

Given an n-dimensional representation $D(g)$ of a group G, a vector $X_1 \varepsilon E^n$ exists such that the set $\{D(g)X_1, \ g\varepsilon G\}$ of vectors spans E^n if and only if every irreducible representation contained in $D(g)$ appears with a multiplicity less than or equal to its dimension.
For a proof see Blake and Mullin [12].

Definition 2.

A representation is said full homogeneous if every irreducible component has a multiplicity equal to its dimension.

The symmetry of a group code is exploited by the configuration matrix. According to the previous definition, it is an M by M matrix of rank n the entries of which are the scalar products $c_{ij} = X_i^T X_j \quad i,j=1,\ldots,M$. It is also of interest to define an extended configuration matrix C^e whenever $|G|>M$. Let $X_g=D(g)X_1$ be the vector produced by the action of the element $g\varepsilon G$. We define the extended configuration matrix as the $|G|$ by $|G|$ Gram matrix whose entries are

$$c_{gg'} = X_g^T X_{g'} \qquad g,g' \varepsilon G$$

Since $H\neq\{e\}$, the vectors of the set $S(G)X_1$ are not all distinct; in fact the same vector appears with multiplicity $|H|$.
The following theorem illustrates the shape and structure of configuration matrices which rely in depth on the associated group.

Theorem 5.

The rows of any configuration matrix of a group code are permutations of the first one.

This applies to both extended and not extended configuration matrices. For a proof see [3] and [10].

It is not hard to verify that the extended C^e configuration matrix is the Kronecker product of C by a matrix J, (possibly with a re-ordering of rows and columns):

$$C^e = C \otimes J$$

where J is a convenient matrix of which all entries are 1s.

The importance of the configuration matrix C of a group codes, was enhanced by Slepian's proof, [3], that it is possible to recover the vectors of the code from C. Let $P_H(g)$, $g \in G$, denote the permutation matrices of the right permutation representation of G induced by its subgroup H; let AG(H) be the group algebra of G generated by these permutation matrices, and let AZ(H) be the centralizing algebra of AG(H). We have the following theorems.

Theorem 6.

The extended configuration matrix of a group code can be written as the sum

$$C^e = \Sigma_g c(g)\, L(g)$$

where L(g), $g \in G$, are the permutation matrices of the left regular permutation representation of G.

Theorem 7.(Slepian)

The extended configuration matrix commutes with all the permutation matrices of the right regular permutation representation of G, i.e. C^e belongs to the centraling algebra of the group algebra of the right regular permutation matrices.

The configuration matrices of different group codes generated by diffe-

rent irreducible representations of the same group G may originate an orthogonal basis in the regular group algebra AG({e}), as stated in the following theorem due to Blake.

Theorem 8.

Let D(g) and D'(g) be real irreducible representations of the finite group G of dimensions n_i and n_j, respectively, and C_i and C_j the configuration matrices of the group codes $\{D(g)X_i,\ g\in G\}$ and $\{D'(g)X_j,\ g\in G\}$, respectively. Then

i) if D(g) and D'(g) are not equivalent, then $C_i\ C_j = 0$ for any X_i and X_j;

ii) if D(g) = D'(g) and $X_i = X_j$, then $(C_i)^2=(G/n_i)\ \|X_i\|^2\ C_i$.

For a proof see Blake and Mullin [12].

Furthermore special structures of the configuration matrix may uniquely characterize the group code.

Theorem 9.(Blake)

Let us consider the configuration matrix C of an [M,n] code in which all entries of the first row are distinct.

Then C is the configuration matrix of a group code if and only if:

i) its rows are permutations of the first one;

ii) M is a power of 2, i.e. $M=2^S$;

iii) in the decomposition

$$C=\sum c_i\ P_i$$

the matrices P_i are permutation matrices of order two and commute with each other.

Moreover $n\geq s$ and the group generating the code is commutative of type $(1,1,\ldots,1)$.

Now we can devise a general theorem concerning the conditions for a given Gram matrix to be the configuration matrix of a group code. However the formulation of such general conditions may be quite unsati-

sfactory, because they lack either classical mathematical fascination or practical utility. It is a challenging question to find more pleasant and possibly useful conditions.

Theorem 10.

A Gram matrix C is the configuration matrix of a group code if and only if

i) rows of C are permutations of the first one;

ii) a matrix J, all entries of which are 1s and the order of which is not greater than (M-1)!, exists such that the matrix $C'=C \otimes J$ commutes with all matrices of a right regular representation of a group G.

See [10] for a proof.

We stop here the presentation of Slepian's group codes. In the next section we shall consider an extension that will include multilevel codes which share, of course, the same underlying property of symmetry.

V - GENERALIZED GROUP ALPHABETS

The class of multidimensional alphabets is introduced. Special instances of these codes have been widely used for designing multidimensional signals in combined modulation and coding. Their structure is very rich in symmetries and, as far as we know, most of the signal constellations in actual use, either equienergetic or not, belong to this family.

Definition 3.

Consider a set of K n-vectors $\underline{X} = \{X_1,\ldots,X_K\}$, called the initial set, and L orthogonal n x n matrices $S_1,\ldots, S_L$ that form a representation S(G) of the group G. The set of vectors $S(G)X_1, \ldots, S(G)X_K$ obtained from the action of S(G) on the vectors of the initial set is called a Generalized Group Alphabet, and from now on shortened to GGA.

Definition 4.

A GGA is called separable if the vectors of the initial set are transformed by S(G) into either disjoint or coincident vector sets, i.e.,

$$S(G)X_j \cap S(G)X_k = \begin{cases} \emptyset & j \neq k \\ S(G)X_j & j = k \end{cases}$$

Since an orthogonal matrix transforms a vector into one with the same length, the signals associated with a GGA have as many energy levels as there are in the initial set.

Definition 5.

A GGA is called regular if the number of vectors in each subalphabet $S(G)X_j$, $j=1,\ldots,K$, does not depend on j, i.e., each vector of the initial set is transformed by S(G) into the same number of distinct vectors. A regular GGA is called strongly regular if each set $S(G)X_j$ contains exactly L distinct vectors.

The following result stems directly from the definitions.

Theorem 11.

The number M of vectors in a regular GGA is a multiple of K. If GGA is strongly regular, then M=KL.

We consider now some distance properties of the elements of a GGA. Choose a partition of a GGA into m subsets $\underline{Z}_1$, $\underline{Z}_2,\ldots,$ $\underline{Z}_m$. For each subset $\underline{Z}_i$, we can define the intradistance set as the set of all the Euclidean distances among pairs of vectors in $\underline{Z}_i$. For any pair of distinct subsets $\underline{Z}_i$, $\underline{Z}_j$, we define their interdistance set as the set of all the Euclidean distances between a vector in $\underline{Z}_i$ and a vector in $\underline{Z}_j$.

Definition 6.

The partition of a separable GGA into m subsets $\underline{Z}_1,\ldots,\underline{Z}_m$ is called fair if all the subsets are distinct, include the same number of vectors and their intradistance sets are equal.

We shall now present a constructive method to generate fair partitions of a GGA. Consider the generating group S(G) of the GGA, one of its subgroups, say S(H), and the partition of S(G) into left cosets of S(H). We have the following result.

Theorem 12.

If the left cosets of the subgroup S(H) are applied to the initial set of a strongly regular GGA, this procedure results in a fair partition of the GGA. Under the same hypotheses, if S(H) is a normal subgroup, then left and right cosets give rise to the same fair partition.
For a proof see [11].

The condition of strong regularity of the GGA can be removed: but in this case it may happen that different cosets generate the same element of the partition. Hence, some of the cosets must be removed from consideration. Moreover, notice that if S(H) is a normal subgroup of S(G), then we do not need to distinguish between left or right coset partitions. On the contrary, if S(H) is not normal, the partitions obtained from right cosets may not be fair, as it can be shown by a counterexample. In some cases, we are interested in further partitioning every element $\underline{Z}_i$ in the same number of subsets. This leads to the concept of a chain partition, that is the GGA is partitioned in subsets which in turn are partitioned in the same number of sub-subsets, and so on. We call level of a subset in the chain partition the number of inclusions beetwen the given subset and the whole group code.

Definition 7.

The chain partition of a separable GGA is called fair if any two elements of the partition at the same level of the chain include the same number of vectors and have equal intradistance sets.

For fair chain partitions we have the following theorem.

Theorem 13.

Consider a strongly regular GGA, and a chain of subgroups of its generating group S(G), that is

$$S(H_1) \subset S(H_2) \subset S(H_3) \subset \ldots \subset S(H_s) = S(G) \quad .$$

Use H_{s-1} and its left cosets to generate a partition of GGA. Then, use H_{s-1} and its left cosets in H_s to further partition all the sets of the previous partition. Repeat the procedure with H_{s-2}, and so on, until H_1 and its left cosets in H_2 are used. The resulting chain partition of GGA is fair.

A theorem concerning the interdistance sets sheds some further light on the symmetry properties of GGA's.

Theorem 14.

Let H be a normal subgroup of G. The partition of a strongly regular GGA obtained by applying the left cosets of H to the initial set $\underline{X}$ has the following property: the interdistance set associated with any two cosets, say S_1H and S_2H, is a function only of the coset S_3H, where $S_3 = S_1^{-1}S_2$, and not of S_1, S_2 separately.
For a proof see [11].

We conclude this section by showing how GGAs, in particular group codes, can be used in conjunction with error control codes to exploit the channel capacity further. We shall illustrate first the joint use of multidimensional alphabets and block codes, thus we will describe how the signal alphabets are paired to convolutional (trellis) codes.

Imai and Hirakawa [33] and recently Ginzburg [31] have described constructions which make it possible to design set of signals with a regular structure and with an arbitrary minimum distance as insured by the algebraic properties of block codes. Ginzburg's construction considers L block encoders $C_1, C_2, \ldots, C_L$ which accept source symbols, and output L blocks $(q_{1i}, q_{2i}, \ldots, q_{Ni})$, $i=1,\ldots,L$, of N symbols each. The modulator f maps each L-tuple $(q_{j1}, \ldots, q_{jL})$, $j=1,\ldots,N$, into the vector

$$X_j = f(q_{j1}, \ldots, q_{jL}), \quad j = 1, \ldots, N$$

chosen from a GGA of $M=M_1 \ldots M_L$ elements. This mapping is obtained as follows. In GGA we define a system of L partitions such that each class of the ℓ-th partition includes M_ℓ classes of the $(\ell-1)$-th partition. Each class will consist of $M(\ell)=M_1 M_2 \ldots M_\ell$ signals. By numbering the classes of the $(\ell-1)$-th level occurring in a class of the ℓ-th level we can obtain a one-to-one mapping of the set of classes of the $(\ell-1)$-th partition onto the set of integers $\{0,\ldots,M_\ell-1\}$. Therefore, if q_{ij} are chosen in the set $\{0,\ldots,M_\ell-1\}$, $\ell=1,\ldots,L$, any L-tuple $(q_{j1}, \ldots, q_{jL})$ defines a unique value of the j-th elementary signal $X_j=f(q_{j1}, \ldots, q_{jL})$.

We shall now see how an Ungerboeck code can be designed using GGA. The procedure suggested in [47] and called "mapping by set partitioning", can be achieved by the notion of fair partition, which represents a systematic generalization of that concept.

Each coded symbol depends on $k+\nu$ source bits, namely the block $\tau=(a_1, \ldots, a_k)$ of k bits generated by the source, plus ν bits preceding this block. The ν bits determine one of the $N=2^\nu$ states of the encoder, say $\sigma = (a_{k+1}, \ldots, a_{k+\nu})$, $a_n=0,1$. The encoder state for the next coded symbol is obtained by shifting the a_n's k places to the right, dropping the right-most k bits and inserting on the left the most recent k source bits. The encoded symbol X_j, which is an element of a GGA, depends on τ and σ and, in this framework, the encoding procedure

can be described using a trellis and by assigning to the branches outgoing from each node the set of symbols obtained from a fair partition of a GGA.

VI - THE INITIAL VECTOR PROBLEM

The minimum distance is a relevant factor to define the code performance on noisy channels because it is a fact that distant signals are hard to confuse as an effect of the noise. Moreover monotone decreasing functions of the minimum distance constitute an upper bound to the error probability. It follows that codes with large minimum distances are desirable, and in particular the choice of Slepian's group codes with the greatest minimum distance leads to the initial vector problem which is also interesting from a geometrical point of view.

The initial vector problem for group codes can be stated as follows: given a finite group S(G) of orthogonal matrices that generates a group code [M,n] by operating on an initial unit vector X, among all such vectors X find out the vector X_o for which the minimum distance is the greatest possible. We have to find the maximum of the minimum of the distances, i.e. to determine a kind of saddle point with respect to the continuous variable X and discrete variable g:

$$\max_{X} \left[\min_{g \neq g'} d(D(g')X, D(g)X) \right]$$

where the maximum is taken over all the vectors of R^n with the constraints $\|X\|=1$ and $S(H)X=X$. S(H) is a subgroup of S(G), possibly $H=\{e\}$. At the present time no general solution is known. The problem has been solved for many classes of group codes and for codes generated by special representations. Djokovic and Blake, [25], settled the case of full homogeneous component; Downey and Karlof found all the optimal group codes in three dimensions [28]; Biglieri and Elia identified the

optimal initial vector for Variant I permutation codes, [9], and showed that for cyclic codes [8] as well as for abelian codes the optimal initial vector is obtained by solving a linear programming problem. Nevertheless, the evidence so far is that the problem cannot have, in general, a closed form solution.

We do not digress on the meaning of "solution", but we adopt the pragmatic view that for practical purposes any kind of numerical solutions should be regarded as a valid one.

For computational approaches the initial vector problem can be stated, in general, as a mathematical problem with a quadratic objective subjected to quadratic constraints, [37].

Let d_0^2 be the minimum square distance. The optimal initial vector X_1 is the solution to:

$$d_0^2 = \text{Max Min } d^2(D(g)X_1, X_1)$$

where the maximum is taken over all unit vectors and the minimum is on all elements $g \in G$ different from the identity.

For any unit vector X and unitary matrix D(g), we have

$$d^2(D(g)X,X) = 2 - 2(D(g)X,X).$$

Thus maximizing the minimum distance is equivalent to minimizing the maximum inner product. We may assume the maximum inner product positive and equal to r^2. Let $Y=(1/r)X_1$. Then, for all non identity elements of G, $(D(g)Y,Y) \leq 1$ and $(Y,Y)=1/r^2$. Hence Y is a solution to:

Find Max (Y,Y)

subject to $(D(g)Y,Y) \leq 1$ whenever g is not the identity in G.

The problem of the initial set of vectors for GGA is more complicated, of course, than for group codes because more than one vector is to be found and different objectives may motivate the choice. In this case one formulation of the initial set vector problem is the following:

> Given S(G) find a set $\{X_1, \ldots, X_K\}$ of K n-dimensional vectors with average square norm equal to E, such that the generated GGA is regular and such that the minimum distance is as large as possible.

Here we do not treat the subject further, as the discussion would be very long. For example GGA used in conjuction with error control codes hopefully must have the maximum possible minimum intradistance associated to a given fair partition.

In this context the open problems are countless; the few known solutions either are heuristic or obtained by hand manipulations. Much work must still be done.

VII - THE CONSTRUCTIVE VIEW

One important intent of the group code theory is to produce good point constellations for the design of digital signals to be used in data transmission, vector quantization, pattern recognition or in many other fields. A second and ambitious objective of this theory is the systematic classification and construction of all regular point constellations in n-dimensional spaces. Before discussing the capabilities of the constructive methods of group coding theory, we present three interesting point constellations that have large minimum distances and provide a good instance of this matter.

The first example is given by the [8,3] group code which is the classical constellation shown in Fig.2, (edges connect points at minimum distance), that has a minimum distance slightly greater than the cube. It is generated by the action of the representation of the cyclic group C_8.

The group is generated by:

$$D(g) = (-1)^h \oplus \begin{pmatrix} \cos(\pi h/4) & \sin(\pi h/4) \\ -\sin(\pi h/4) & \cos(\pi h/4) \end{pmatrix}$$

The initial vector is $(\sqrt{(1/(2\sqrt{2}+1))}, \sqrt{(2\sqrt{2}/(2\sqrt{2}+1))}, 0)$

The minimum distance is $d^2_{min} = 4/(2 + 1/\sqrt{2}) > 4/3$

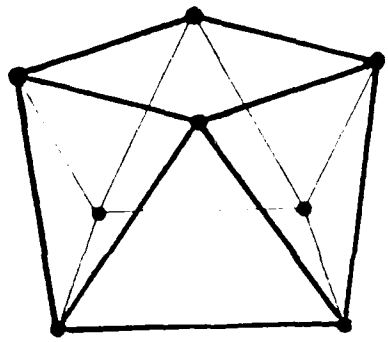


Fig.2

The second example is a not regular and not equienergetic GGA having 14 points in 3 dimensions. The configuration shown in Fig.3, is generated by the action of a representation of the group of the cube

$$C_2 \times C_2 \times C_2 \times S_3 .$$

The initial set is {(u, 0, 0), (v, v, v)}, where

$$v = \sqrt{7}\,(7 - 2\sqrt{2})/123 \qquad u = \sqrt{7}\,(13 + 8\sqrt{2})/123$$

The minimum distance is $d^2_{min} = 28\,(7 - 2\sqrt{2})/123 = 0.9496$ and it is significantly greater than 0.93386, the minimum distance of the best known spherical 14 point configuration.

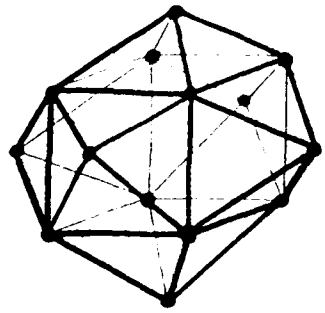


Fig.3

Finally, the third and last example is the [16,4] group code generated by the action of a representation of the abelian group $C_2 \times C_8$. The configuration is shown in Fig.4. The representation is generated by

$$D(g) = (-1)^k \oplus (-1)^{h+k} \oplus \begin{pmatrix} \cos(\pi h/4) & \sin(\pi h/4) \\ -\sin(\pi h/4) & \cos(\pi h/4) \end{pmatrix} \qquad \begin{matrix} k=1,2 \\ h=1,\ldots,8 \end{matrix}$$

The initial vector is $(\sqrt{((\sqrt{2}-1)/2)}, \sqrt{((\sqrt{2}-1)/2)}, \sqrt{(2-\sqrt{2})}, 0)$.

The minimum distance is $d^2_{min} = 2\,(2-\sqrt{2}) = 1.1716$

Note that one of the most used point constellations, the two dimensional 16-QAM has minimum square distance 2/5= 0.4.

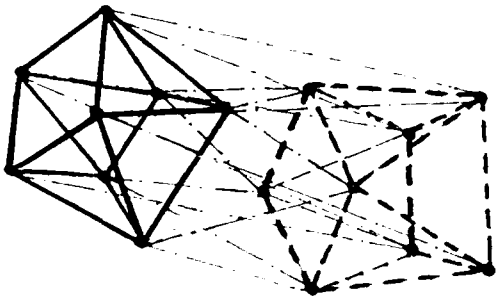


Fig.4

The ingredients involved in the constructive aspect of group codes are groups, matrices and imagination. Four remarkable achievements are partially responsible for:

1) an old theorem by Jordan stating that the number of finite groups with trivial maximal normal abelian subgroup, which have an irreducible representation of dimension n, is finite and upper bounded by $b(n)= n!\ 6^{\pi(n)\,(n-1)+2}$, where $\pi(n)$ counts the number of primes less than n;
2) the recent classification of all finite simple groups;
3) the fact that the number of finite groups of given order is finite;

4) the complete classification of all commutative groups as well as their representations.

Finite simple groups, Galois' fundamental discovery, are instrumental in building up all other groups and their representations. Abelian groups together with finite group having trivial center can be used to classify all groups which have a representation in n-dimensional spaces. In this context it is useful to recall the outstanding theorem of the classification of finite groups, completed in 1981. This theorem resulted from the global efforts of several hundred mathematicians from all-over the world over a period of 100 years. It is remarkable by itself and relevant to the classification of group codes.

Theorem 15. [20]

The finite simple groups are to be found among:

i) the cyclic groups C_p of prime order p.

ii) the alternating groups A_n of degree n at least 5.

iii) the Chevalley groups

iv) the Tits group

v) the 26 sporadic simple groups.

The Mathieu group, usually denoted by M_{24}, played a central role in the discovery of all 26 sporadic groups. M_{24} is also important in the theory of error-correcting codes, because it is the automorphism group of the Golay code (24,12,8), the only binary perfect multiple error correcting code; see [39,49,21].

Even if it is not necessary to resort to the above definitive theorem, simple groups play a basic role in group codes.

Theorem 16.

Let us consider a [M,n] group code generated by a group G through its representation D(g). If M is a prime number then the group code is generated by a cyclic subgroup C_M of G.

Theorem 17.

No [M,n] group codes exists if M is an odd prime and n is odd.

Theorem 18.

A [M,n] group code can be constructed using representations of a cyclic group provided that either

i) n is even and M>2

or

ii) n is odd and M is even.

Theorem 19.

The number of [M,n] group codes, generated by irreducible representations of groups with trivial maximal normal abelian subgroup is finite and bounded by a function of n alone.

Concluding this section we remark that the problem of the existence of group codes for every M and n is very interesting as it concerns the existence of regular configurations of points on n-dimensional spheres, and generalizes the vertex configurations of regular polytopes.
We can summarize the results as follows:

a)	n even	M≥n+1	at least one group code generated by a cyclic group of order M exists
b)	n odd,	M even≥n+1	at least one group code generated by a cyclic group of order M exists
c)	n even	M odd prime	only one group code generated by the cyclic group of order M exists
d)	n odd,	M odd prime	no group code exists
e)	n = 3,	any M	all group codes have been classified by Downey and Karlof. No group codes with M odd exist.

The definitive classification of all group codes is far from complete, so that many open problems and conjectures still deserve attention. Most of these problems are appealing and may produce beautiful results. We recall, by way of sample, two interesting problems that are still open:

- One group code in dimension 5 with M=15 is known to exist, [26]. It is conjectured that it is the only group code in five dimensional space with an odd number of points.
- Brauer [15] and his school have reached the classification of all groups having an irreducible representation in dimension 4 and 5. It would be interesting to find out all group codes in dimension 4 (the useful dimension for today's applications).

  The determination of all group codes [M,5] would also be interesting as well as the classification of [M,7]. The latter is possible due to the complete list of groups with irreducible representation in dimension 7 obtained by Wales [50, 51, 52].

VIII. CONCLUSIONS

The impact of ancient and modern mathematical concepts on manipulation, transmission and storing of information has made a science of fine, intelligent but scattered techniques.

In this paper we reported on group code theory as an application of general results originated from the ancient geometry. The geometric view provides the appropriate framework for dealing with digital signal processing, signal design, vector quantization and in general communication systems. To enhance the importance of this concept in communication we also considered the combination of these alphabets with block or trellis codes. We have not described the interesting connection of lattices, group codes and combined modulation and coding, this beautiful subject is thoroughly developed in the fundamental book [21] by

Conway and Sloane.

In this paper no essentially new results were proposed. However we hope that the presentation of a topic which is earning a prominent position with increasing applications in the new global communication system will be of some interest, especially to young researchers who are looking for fruitful areas of research with high scientific content and useful applications.

We think that group code theory, which may be credited of a long history dated back to ancient regular polyhedra, is a good example of Feller's conception of mathematics [56]. In fact we wish to conclude with Feller's words:

> "The manner in which mathematical theories are applied does not depend on preconceived ideas: it is a purposeful technique depending on, and changing with experience".

REFERENCES

[1] D.Slepian, "Bounds on Communication", Bell System Technical Journal, vol.42, May 1963, pp.681-707.

[2] D. Slepian, "A Class of Binary Signaling Alphabets", BSTJ, n.35, pp.203-234, January 1956.

[3] D.Slepian, "Group codes for the Gaussian channel", Bell System Technical Journal, vol.47, April 1968, pp.575-602.

[4] D.Slepian, "On neighbor Distances and Symmetry in Group Codes", IEEE Trans. on Information Theory, vol.IT-17, September 1971, pp.630-632.

[5] D. Slepian, "Permutation Modulation", Proc. of the IEEE, March 1965.

[6] D. Slepian, "Some comments on Fourier Analysis, Uncertainty and Modelling", SIAM Rew., vol.25, n.3, July 1983.

[7] E.Biglieri amd M.Elia, "On the existence of group codes for the Gaussian channel", IEEE Trans. on Inform. Theory, vol.IT-18, May 1972, pp.399-402.

[8] E.Biglieri, and M.Elia, "Cyclic-group codes for the Gaussian channel", IEEE Trans. on Inform. Theory, vol.IT-22,n.5, September 1976, pp.624-629.

[9] E.Biglieri and M.Elia, "Optimum Permutation Modulation Codes and Their Asymptotic Performance",IEEE Trans. on Information Th., vol.IT-22, n.6, November 1976, pp.751-753.

[10] E.Biglieri and M.Elia, "Configuration matrices of Group Codes for the Gaussian Channel", Int. Symp. on Inform. Theory, Cornell, USA, November 1977.

[11] E.Biglieri and M.Elia, "Multidimensional Modulation and Coding for Bandlimited Channels",IEEE Trans. on Inform. Theory, to be published.

[12] I.F.Blake and R.C.Mullin, "The Mathematical Theory of Coding", Academic Press, New York, 1975.

[13] I.F.Blake, "Distance properties of Group Codes for the Gaussian Channel", SIAM Journal of Applied Math., vol.23, No.3, 1972.

[14] I.F.Blake, "Configuration matrices of group codes", IEEE Trans. on Inform. Theory, vol.IT-20, n.1, January 1974, pp.95-100.

[15] R. Brauer, "Uber endliche lineare Gruppen von Primzahlgrad", Mathematical Annalen, 169, 1967, pp.73-96.

[16] W.Burnside, "Theory of groups of Finite Order", Dover, New York, 1955.

[17] M.Burrow, "Representation Theory of Finite Groups", Academic Press, New York, 1965.

[18] A.R.Calderbank and J.E.Mazo, "A new description of trellis codes", IEEE Trans. on Inform. Theory, vol.IT-30, November 1984, pp.784-791.

[19] A.R.Calderbank, and N.J.A.Sloane, "Four-Dimensional Modulation with an Eight-State Trellis Code", AT&T Tech. Journal, Vol.64, No.5, May-June 1985, pp.1005-1018.

[20] J.H.Conway, R.T.Curtis, S.P.Norton, R.A.Parker, R.A.Wilson, "ATLAS of finite groups", Clarendon Press, Oxford, 1985

[21] J.H.Conway and N.J.A. Sloane, "Sphere-packing, Lattices and Groups", Springer Verlag, New York, 1987, to appear.

[22] H.M.S. Coxeter, "Regular Polytopes", Dover, New York, 1973.

[23] H.M.S. Coxeter, "Regular Complex Polytopes", Cambridge University press, London, 1974.

[24] C.W.Curtis and I.Reiner, "Representations Theory of Finite Groups and Associative Algebras", Wiley, New York, 1966.

[25] D.Djokovic and I.Blake, "An Optimization problem for Unitary and orthogonal Representations of Finite Group", Trans. of the American Math. Soc. 164, 1972.

[26] C.P. Downey and J.K. Karlof, "On the Existence of [M,n] Group Codes for the Gaussian Channel with M and n Odd", IEEE Trans. Inform. Theory, vol.IT-23, no.4, July 1977, pp.500-503.

[27] C.P. Downey and J.K. Karlof, "Odd Group Codes for the Gaussian Channel", SIAM J. Appl. Math., vol.34, no.4, June 1978 pp.715-720.

[28] C.P. Downey and J.K. Karlof, "Computational Methods for Optimal [M,3] Group Codes for the Gaussian Channel", Utilitas Mathematica, vol. 18, March 1980, pp.51-70.

[29] C.P. Downey and J.K. Karlof, "Group Codes for the Gaussian Broadcast Channel with two receivers", IEEE Trans. Inform. Theory, vol.IT-26, no.4, July 1980, pp.406-411.

[30] L.E. Franks, "Signal Theory", Prentice Hall, 1969.

[31] V.V.Ginzburg,"Mnogomerniye signaly dlya nepreryvnogo kanala" Problemy Peredaci Informacii, n.1, 1984, pp.28-46, (in Russian).

[32] I.Hargittai, "Symmetry: Unifying Human Understanding", Pergamon, 1986.

[33] H.Imai, S.Hirakawa, "A new multilevel coding method using error-correcting codes", IEEE Trans. on Inform. Theory, vol.IT-23, 1977, pp.371-377.

[34] I. Ingemarsson, "Commutative group codes for the gaussian channel", IEEE Trans. on Inform. Theory, vol. IT-19, pp.215-219.

[35] I. Ingemarsson, "On the structure of group codes for the Gaussian channel", Report LiTH-ISY-I-0782, Linkoping University, Sweden, 1986.

[36] I.Jacobs, "Comparison of M-ary modulation systems", Bell System Technical Journal, vol.46, May-June 1967, pp.843-864

[37] J.K. Karlof, "Permutation Codes for the Gaussian Channel", Report of Dpt. Math. Sciences, University of North Carolina, Wilmington, 1987.

[38] R. McEliece, "The Theory of Information and Coding", Addison Wesley, 1977.

[39] F.J.MacWilliams and N.J.A.Sloane, "The Theory of Error-Correcting Codes", Amsterdam: North-Holland, 1977.

[40] A. Papoulis, "The Fourier Integral and its Applications", McGraw-Hill, 1962.

[41] A. Papoulis, "Signal Analysis", New York, McGraw-Hill, 1977.

[42] W.W. Peterson and E.J. Weldon, "Error-Correcting Codes", MIT Press, Cambrdge, 1981.

[43] C.E. Shannon, "A Mathematical Theory of Communications", BSTJ, vol.27, 1948, pt.I pp.379-423, pt.II pp.623-656.

[44] C.E. Shannon, "Probability of Error for Optimal Codes in a Gaussian channel", BSTJ, vol.38, May 1959, pp.611-656.

[45] Shu Lin and D.J. Costello, "Error Control Coding: Fundamentals and Applications", Prentice-Hall, Englewood Cliffs, New Jersey, 1983.

[46] N.J.A.Sloane, "Tables of Sphere Packing and Sperical Codes", IEEE Trans. on Inform. Th., vol.IT-27, n.3, May 1981, pp.327-338.

[47] G.Ungerboeck,"Channel coding with multilevel/phase signals" IEEE Trans. on Inform. Theory, vol.IT-28, January 1982, pp.55-67.

[48] B.L.van der Waerden, "Modern Algebra", vol.1/2, Ungar, New York, 1953.

[49] J.H.Van Lint, "Introduction to Coding Theory", New York, Springer Verlag, 1982.

[50] D.B.Wales, "Finite Linear Groups of prime degree", Canadian Journal of Mathematics, 21, 1969, pp.1025-1041.

[51] D.B.Wales, "Finite Linear Groups of degree seven, I", Canadian Journal of Mathematics, 21, 1969, pp.1042-1066.

[52] D.B.Wales, "Finite Linear Groups of degree seven, II", Pacific Journal of Mathematics, vol.34, N.1, 1970, pp.207-235.

[53] H.Weyl, "Symmetry", Princeton University Press, Princeton, 1952.

[54] J.Wozencraft and I.Jacobs, "Principles of Communication Engineering", Wiley, New York, 1965.

[55] E.Zehavi and J.K.Wolf, "On the performance evaluation of trellis codes", IEEE Trans. on Information Theory, vol.IT-33, n.2, March 1987,pp.196-202.

[56] W.Feller, "An Introduction to Probability Theory and its Applications", vol. I, Wiley, New York, 1968.

END

DATE

FILMED

DTIC

4/88